Groupe de travail Réseau
Request for Comments : 4555
Catégorie : Sur la voie de la normalisation

P. Eronen, éditeur, Nokia
juin 2006
Traduction Claude Brière de L'Isle

Protocole IKEv2 de mobilité et de rattachement multiple (MOBIKE)

Statut du présent mémoire

Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

Le présent document décrit le protocole MOBIKE, une extension de mobilité et de multi rattachements à l'échange de clés Internet (IKEv2, *Internet Key Exchange*). MOBIKE permet de changer les adresses IP associées aux associations de sécurité IPsec en mode tunnel et IKEv2. Un client de réseau privé virtuel (VPN, *Virtual Private Network*) pourrait utiliser MOBIKE pour garder active la connexion avec la passerelle de VPN tout en se déplaçant d'une adresse à une autre. De même, un hôte multi rattachements pourrait utiliser MOBIKE pour déplacer le trafic sur une interface différente si, par exemple, celle utilisée actuellement cesse de fonctionner.

Table des matières

1. Introduction

1.1 Motivation

IKEv2 est utilisé pour effectuer l'authentification mutuelle, ainsi que l'établissement et la maintenance des associations de sécurité (SA, *Security Association*) IPsec. Dans le protocole IKEv2 de base [RFC4306], les SA IKE et les SA IPsec en mode tunnel sont créées implicitement entre les adresses IP qui sont utilisées quand la IKE_SA est établie. Ces adresses IP sont alors utilisées comme adresses externes (d'en-tête de tunnel) pour les paquets IPsec en mode tunnel (les SA IPsec en mode transport sortent du domaine d'application du présent document). Actuellement, il n'est pas possible de changer ces adresses après la création de la SA IKE.

Il y a des scénarios où ces adresses IP peuvent changer. Un exemple est la mobilité : un hôte change son point de rattachement au réseau et reçoit une nouvelle adresse IP. Un autre exemple est un hôte multi rattachements qui voudrait changer pour une interface différente si, par exemple, celle actuellement utilisée cesse de fonctionner pour une raison quelconque.

Bien que le problème puisse être résolu en créant de nouvelles SA IKE et IPsec quand les adresses ont besoin d'être changées, ce peut n'être pas optimal pour plusieurs raisons. Dans certains cas, créer une nouvelle SA IKE peut exiger une interaction avec l'utilisateur pour l'authentification, comme d'entrer un code à partir d'une carte à jeton. Créer de nouvelles SA implique souvent des calculs coûteux et éventuellement un grand nombre d'allers-retours. Pour ces raisons, un mécanisme de mise à jour des adresses IP des SA IKE et IPsec existantes est nécessaire. Le protocole MOBIKE décrit dans le présent document fournit un tel mécanisme.

Le principal scénario pour MOBIKE est l'activation d'un accès distant d'utilisateur de VPN pour passer d'une adresse à une autre sans rétablir toutes les associations de sécurité avec la passerelle de VPN. Par exemple, un utilisateur pourrait partir d'un Ethernet fixe au bureau et ensuite déconnecter la tablette et passer au LAN sans fil du bureau. Quand l'utilisateur quitte le bureau, la tablette pourrait commencer d'utiliser le service général radio par paquets (GPRS, *General Packet Radio Service*) ; quand l'utilisateur arrive chez lui, la tablette pourrait passer au LAN sans fil du domicile. MOBIKE met seulement à jour les adresses externes (d'en-tête de tunnel) des SA IPsec, et les adresses et autres sélecteurs de trafic utilisés à l'intérieur du tunnel restent inchangés. Donc, la mobilité peut être (presque) invisible aux applications et à leurs connexions qui utilisent le VPN.

MOBIKE prend aussi en charge des scénarios plus complexes où la passerelle de VPN a aussi plusieurs interfaces réseau : ces interfaces pourraient être connectées à différents réseaux ou FAI, elles peuvent être un mélange d'adresses IPv4 et IPv6, et les adresses peuvent changer dans le temps. De plus, les deux parties pourraient être des passerelles de VPN qui relaient le trafic pour d'autres parties.

1.2 Portée et limites

Le présent document se concentre sur le scénario principal mentionné ci-dessus et prend seulement en charge les SA IPsec en mode tunnel.

La prise en charge de la mobilité dans MOBIKE permet aux deux parties de se déplacer, mais ne fournit pas de mécanisme de "rendez vous" qui permettrait un mouvement simultané des deux parties ou la découverte des adresses quand la SA IKE est établie. Donc, MOBIKE convient mieux aux situations où l'adresse d'au moins un des points d'extrémité est relativement stable et peut être découverte en utilisant des mécanismes existants comme le DNS (voir au paragraphe 3.1).

MOBIKE permet aux deux parties d'être multi rattachements ; cependant, seulement une paire d'adresses est utilisée à la fois pour une SA. En particulier, l'équilibrage de charge sort du domaine d'application de la présente spécification.

MOBIKE suit les pratiques de IKEv2 lorsque un message de réponse est envoyé à la même adresse et accès d'où la demande a été reçue. Cela implique que MOBIKE ne fonctionne pas sur des paires d'adresses qui fournissent seulement une connexité unidirectionnelle.

Les traducteurs d'adresse réseau (NAT, *Network Address Translator*) introduisent des limitations supplémentaires au delà de celles mentionnées ci-dessus. Voir les détails au paragraphe 2.3.

La version de base du protocole MOBIKE ne couvre pas tous les futurs scénarios d'utilisation potentiels, comme le mode transport, l'application à la sécurisation de SCTP, ou les optimisations désirables dans des circonstances spécifiques. De futures extensions pourront être définies ultérieurement pour prendre en charge des exigences particulières. Prière de consulter le document de conception de MOBIKE [RFC4621] pour plus d'informations et les raisons de ces limitations.

1.3 Terminologie et notation

Quand des messages qui contiennent des charges utiles IKEv2 sont décrits, les charges utiles facultatives sont montrées entre guillemets (par exemple, "[FOO]"), et un signe plus indique qu'une charge utile peut être répétée une ou plusieurs fois (par exemple, "FOO+"). Pour donner le contexte, certains diagrammes montrent aussi quelles charges utiles IKEv2 existantes vont normalement être incluses dans les échanges. Ces charges utiles sont montrées à des fins d'illustration seulement ; voir dans la [RFC4306] une description d'autorité.

Quand le présent document décrit la mise à jour des adresses de source/destination d'une SA IPsec, il signifie la mise à jour de l'état relatif à IPsec afin que les paquets sortants d'en-tête d'authentification (AH, *Authentication Header*) de charge utile d'encapsulation de sécurité (ESP, *Encapsulating Security Payload*) utilisent ces adresses dans l'en-tête de tunnel. Selon la façon dont les divisions nominales entre la base de données d'associations de sécurité (SAD, *Security Association Database*) la base de données de politique de sécurité (SPD, *Security Policy Database*) et la base de données d'autorisations d'homologues (PAD, *Peer Authorization Database*) décrites dans la [RFC4301] sont en fait mises en œuvre, une mise en œuvre peut avoir plusieurs endroits différents à mettre à jour.

Dans le présent document, le terme "initiateur" signifie la partie qui a à l'origine initié la première SA IKE (dans une série de plusieurs SA IKE possibles qui changent de clés) ; le "répondant" est l'autre homologue. Pendant la durée de vie de la SA IKE, les deux parties peuvent initier des échanges INFORMATION ou CRÉER_UNE_SA_FILLE ; dans ce cas, les termes "initiateur de l'échange" et "répondant de l'échange" sont utilisés. Le terme "initiateur d'origine" (qui dans la [RFC4306] se réfère à la partie qui a commencé le dernier changement de clé de SA IKE) n'est pas utilisé dans le présent document.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Vue d'ensemble du protocole

2.1 Fonctionnement de base

MOBIKE permet aux deux parties d'avoir plusieurs adresses, et il y a jusqu'à N*M paires d'adresses IP qui pourraient être utilisées. La décision d'utiliser une de ces paires doit prendre en compte plusieurs facteurs. D'abord, les parties peuvent avoir des préférences quant à l'interface qui devrait être utilisée du fait, par exemple, des performances et des coûts. Ensuite, la décision est contrainte par le fait que certaines des paires peuvent ne pas fonctionner à cause de versions IP incompatibles, de pannes dans le réseau, de problèmes à la liaison locale à l'une ou l'autre extrémité, et ainsi de suite.

MOBIKE résout ce problème par une approche simple : la partie qui initie la SA IKE (le "client" dans un scénario de VPN d'accès distant) est responsable de décider quelle paire d'adresses est utilisée pour les SA IPsec et de collecter les informations nécessaires pour prendre cette décision (comme de déterminer quelles paires d'adresses fonctionnent ou pas). L'autre partie (la "passerelle" dans un scénario de VPN d'accès distant) dit simplement à l'initiateur quelles adresses il a, mais ne met pas à jour les SA IPsec avant d'avoir reçu un message de l'initiateur lui disant de le faire. Cette approche s'applique aux adresses dans les SA IPsec ; dans le cas de SA IKE, l'initiateur de l'échange peut décider quelles adresses sont utilisées. Prendre la décision chez l'initiateur est cohérent avec la façon dont fonctionne le IKEv2 normal : l'initiateur décide des adresses qu'il utilise quand il contacte le répondant. Cela a aussi un sens, en particulier quand l'initiateur est un nœud mobile : il est dans une meilleure position pour décider laquelle de ses interfaces réseau devrait être utilisée pour le trafic vers l'amont et vers l'aval.

Les détails de la façon exacte dont l'initiateur prend la décision, de quelles informations sont utilisées pour la prendre, de comment les informations sont collectées, comment les préférences affectent la décision, et de quand une décision doit être changée sortent largement du domaine d'aplication de MOBIKE. Cela ne signifie pas que ces détails sont sans importance : au contraire, ils sont probablement cruciaux dans tout système réel. Cependant, MOBIKE n'est concerné par ces détails que dans la mesure où ils sont visibles dans les messages IKEv2/IPsec échangés entre les homologues (et donc doivent être normalisés pour assurer l'interopérabilité).

Beaucoup de ces questions ne sont pas spécifiques de MOBIKE, mais sont communes à l'utilisation des hôtes existants dans des environnements dynamiques ou avec des protocoles de mobilité comme IP mobile [RFC3344], [RFC3775]. Un certain nombre de mécanismes existent déjà ou sont en cours de développement pour traiter ces questions. Par exemple, des mécanismes de couche de liaison et de couche IP peuvent être utilisés pour tracer l'état de connexité au sein de la liaison locale [RFC2461] ; la détection du mouvement est spécifiée pour IPv4 et IPv6 dans la [RFC4436], [DNA6], et ainsi de suite.

Naturellement, la mise à jour des adresses des SA IPsec doit prendre en compte plusieurs considérations de sécurité. MOBIKE inclut deux caractéristiques conçues pour traiter ces considérations. D'abord, une vérification "d'acheminement de retour" peut être utilisée pour vérifier les adresses fournies par l'homologue. Cela rend plus difficile d'inonder des tiers avec de grosses quantités de trafic. Ensuite, une caractristique "d'interdiction de NAT" assure que les adresses IP n'ont pas été modifiées par des NAT, des agents de traduction IPv4/IPv6, ou autres appareils similaires. Cette caractéristique n'est activée que quand la traversée de NAT n'est pas utilisée.

2.2 Exemple d'échanges du protocole

Un simple échange MOBIKE dans un scénario mobile est illustré ci-dessous. La notation se fonde sur le paragraphe 1.2 de la [RFC4306]. De plus, les adresses IP et accès de source/destination sont montrés pour chaque paquet : IP_I1, IP_I2, IP_R1, et IP_R2 représentent les adresses IP utilisées par l'initiateur et le répondant.

Initiateur **Répondant**

```
1) (IP_I1:500 -> IP_R1:500)
    HDR, SAi1, KEi, Ni, N(NAT_DETECTION_SOURCE_IP),
        N(NAT_DETECTION_DESTINATION_IP)  ---------------->

                                        <------- (IP_R1:500 -> IP_I1:500)
                                                 HDR, SAr1, KEr, Nr, N(NAT_DETECTION_SOURCE_IP),
                                                 N(NAT_DETECTION_DESTINATION_IP)

2) (IP_I1:4500 -> IP_R1:4500)
    HDR, SK { IDi, CERT, AUTH, CP(CFG_REQUEST),
        SAi2, TSi, TSr, N(MOBIKE_SUPPORTED) }  ------>

                                         <------ (IP_R1:4500 -> IP_I1:4500)
                                                 HDR, SK { IDr, CERT, AUTH, CP(CFG_REPLY),
                                                 SAr2, TSi, TSr, N(MOBIKE_SUPPORTED) }
```

(L'initiateur obtient des couches inférieures l'information que son point et son adresse de rattachement ont changé.)

```
3) (IP_I2:4500 -> IP_R1:4500)
    HDR, SK { N(UPDATE_SA_ADDRESSES),
    N(NAT_DETECTION_SOURCE_IP),
    N(NAT_DETECTION_DESTINATION_IP) } ----->

                                        <------ (IP_R1:4500 -> IP_I2:4500)
                                                 HDR, SK { N(NAT_DETECTION_SOURCE_IP),
                                                 N(NAT_DETECTION_DESTINATION_IP) }
```

(Le répondant vérifie que l'initiateur a donné une adresse IP correcte.)

```
4)                                       <-- (IP_R1:4500 -> IP_I2:4500)
                                                 HDR, SK { N(COOKIE2) }
```

```
   (IP_I2:4500 -> IP_R1:4500)
     HDR, SK { N(COOKIE2) } -------->
```

L'étape 1 est l'échange IKE_INIT normal. Dans l'étape 2, les homologues s'informent l'un l'autre qu'ils prennent en charge MOBIKE. Dans l'étape 3, l'initiateur remarque un changement de sa propre adresse, et en informe le répondant en envoyant une demande INFORMATIONAL contenant la notification UPDATE_SA_ADDRESSES. La demande est envoyée en utilisant la nouvelle adresse IP. À ce point, il commence aussi à utiliser la nouvelle adresse comme adresse de source dans son propre trafic ESP sortant. À réception de la notification UPDATE_SA_ADDRESSES, le répondant enregistre la nouvelle adresse et, si il y est obligé par la politique, effectue une vérification de l'acheminement de retour de l'adresse. Quand cette vérification s'achève (étape 4) le répondant commence à utiliser la nouvelle adresse comme destination de son trafic ESP sortant.

Un autre protocole fonctionnant dans un scénario de multi rattachements est illustré ci-dessous. Dans ce scénario, l'initiateur a une adresse mais le répondant en a deux.

```
     Initiateur                                              Répondant
1) (IP_I1:500 -> IP_R1:500)
     HDR, SAi1, KEi, Ni, N(NAT_DETECTION_SOURCE_IP),
      N(NAT_DETECTION_DESTINATION_IP)  ------------------>

                                          <------- (IP_R1:500 -> IP_I1:500)
                                                   HDR, SAr1, KEr, Nr, N(NAT_DETECTION_SOURCE_IP),
                                                   N(NAT_DETECTION_DESTINATION_IP)

2) (IP_I1:4500 -> IP_R1:4500)
     HDR, SK { IDi, CERT, AUTH, CP(CFG_REQUEST),
     SAi2, TSi, TSr, N(MOBIKE_SUPPORTED) }  ----------------->

                                          <-------- (IP_R1:4500 -> IP_I1:4500)
                                                   HDR, SK { IDr, CERT, AUTH, CP(CFG_REPLY), Sar2, TSi,
                                                  TSr, N(MOBIKE_SUPPORTED), N(ADDITIONAL_IP4_ADDRESS) }
```

(L'initiateur suspecte un problème dans la paire d'adresses actuellement utilisée et vérifie sa vivacité.)

```
3) (IP_I1:4500 -> IP_R1:4500)
     HDR, SK { N(NAT_DETECTION_SOURCE_IP),
      N(NAT_DETECTION_DESTINATION_IP) }  ---------------->

     (IP_I1:4500 -> IP_R1:4500)
     HDR, SK { N(NAT_DETECTION_SOURCE_IP),
     N(NAT_DETECTION_DESTINATION_IP) }  ----------------->

     ...
```

(Finalement, l'initiateur abandonne la paire d'adresses actuelle et vérifie l'autre paire d'adresses disponible.)

```
4) (IP_I1:4500 -> IP_R2:4500)
     HDR, SK { N(NAT_DETECTION_SOURCE_IP),
          N(NAT_DETECTION_DESTINATION_IP) }

                                          <------  (IP_R2:4500 -> IP_I1:4500)
                                                   HDR, SK { N(NAT_DETECTION_SOURCE_IP),
                                                   N(NAT_DETECTION_DESTINATION_IP) }
```

(Cela a fonctionné, et l'initiateur demande à l'homologue de passer aux nouvelles adresses.)

```
5) (IP_I1:4500 -> IP_R2:4500)
     HDR, SK { N(UPDATE_SA_ADDRESSES),
        N(NAT_DETECTION_SOURCE_IP),
        N(NAT_DETECTION_DESTINATION_IP),
```

N(COOKIE2) } ---------->

<---- (IP_R2:4500 -> IP_I1:4500)
HDR, SK { N(NAT_DETECTION_SOURCE_IP),
N(NAT_DETECTION_DESTINATION_IP), N(COOKIE2) }

2.3 MOBIKE et traduction d'adresse réseau

Dans certains scénarios MOBIKE, le réseau peut contenir des NAT ou des filtres de paquets à états pleins (pour faire bref, la suite du présent document décrit simplement des NAT). La caractéristique de traversée de NAT spécifiée dans la [RFC4306] permet à IKEv2 de fonctionner à travers des NAT dans de nombreux cas, et MOBIKE peut développer cette fonctionnalité : quand les adresses utilisées pour les SA IPsec sont changées, MOBIKE peut activer ou désactiver comme nécessaire la traversée de NAT IKEv2.

Néanmoins, il y a quelques limitations parce que les NAT introduisent généralement une asymétrie dans le réseau : seuls les paquets venant de "l'intérieur" causent la création d'un état. Cette asymétrie conduit à des restrictions sur ce que MOBIKE peut faire. Pour donner un exemple concret, considérons une situation où les deux homologues ont seulement une adresse, et où l'initiateur est derrière un NAT. Si l'adresse du répondant change, il doit envoyer un paquet à l'initiateur en utilisant sa nouvelle adresse. Cependant, si le NAT est, par exemple, du type courant "à cône restreint" (voir à la Section 5 de la [RFC3489] une description des différents types de NAT) ceci n'est pas possible. Le NAT va éliminer les paquets envoyés de la nouvelle adresse (sauf si l'initiateur a précédemment envoyé un paquet à cette adresse – ce qu'il ne peut pas faire tant qu'il ne connaît pas l'adresse).

Pour rester simple, MOBIKE ne tente pas de traiter tous les scénarios possibles en rapport avec les NAT. MOBIKE suppose plutôt que si des NAT sont présents, l'initiateur est la partie "derrière" le NAT, et le cas où les adresses du répondant changent n'est pas pleinement pris en charge (ce qui signifie qu'aucun effort particulier n'est fait pour prendre en charge cette fonctionnalité). Les répondants peuvent aussi n'être pas au courant des NAT ou du type spécifique de NAT derrière lequel ils sont. Cependant, quand un changement s'est produit qui va causer une perte de connexité, les répondants MOBIKE vont quand même tenter d'informer l'initiateur du changement. Selon, par exemple, le type exact de NAT, il peut ou non réussir. Cependant, analyser les circonstances exactes où cela va ou non fonctionner n'est pas fait dans le présent document.

3. Échanges du protocole

3.1 Échange initial IKE

L'initiateur est chargé de trouver une paire d'adresses qui fonctionne afin que l'échange IKE initial puisse être mené à bien. Toutes les informations provenant des extensions MOBIKE ne seront disponibles que seulement plus tard, quand l'échange aura suffisamment progressé. Comment exactement les adresses utilisées pour l'échange initial sont découvertes sort du domaine d'application de cette spécification ; les sources normales d'information incluent la configuration locale et le DNS.

Si l'un ou l'autre ou les deux homologues ont plusieurs adresses, certaines combinaisons peuvent ne pas fonctionner. Donc, l'initiateur DEVRAIT essayer diverses combinaisons d'adresses de source et de destination quand il retransmet la demande IKE_SA_INIT.

3.2 Signalisation de la prise en charge de MOBIKE

Les mises en œuvre qui souhaitent utiliser MOBIKE pour une IKE_SA particulière DOIVENT inclure une notification MOBIKE_SUPPORTED dans l'échange IKE_AUTH (dans le cas de plusieurs échanges IKE_AUTH, dans le message contenant la charge utile SA).

Le format de la notification MOBIKE_SUPPORTED est décrit à la Section 4.

3.3 Adresses initiales d'en-tête de tunnel

Quand une SA IPsec est créée, les adresses IP d'en-tête de tunnel (et de l'accès, si on fait une encapsulation UDP) sont prises dans la IKE_SA, et non dans l'en-tête IP du message IKEv2 qui demande la SA IPsec. Les adresses dans la IKE_SA sont initialisées à partir de l'en-tête IP de la première demande IKE_AUTH.

Les adresses sont prises dans la demande IKE_AUTH parce que IKEv2 exige de changer l'accès 500 en l'accès 4500 si un NAT est découvert. Pour simplifier les choses, les mises en œuvre qui prennent en charge cette spécification et la traversée de NAT DOIVENT passer à l'accès 4500 si le correspondant prend aussi les deux en charge, même si aucun NAT n'a été détecté entre eux (de cette façon, il n'est pas nécessaire de changer plus tard l'accès si un NAT est détecté sur un autre chemin).

3.4 Adresses supplémentaires

L'initiateur et le répondant PEUVENT tous deux inclure une ou plusieurs notifications ADDITIONAL_IP4_ADDRESS et/ou ADDITIONAL_IP6_ADDRESS dans l'échange IKE_AUTH (en cas de plusieurs échanges IKE_AUTH, dans le message contenant la charge utile SA). Ici, "ADDITIONAL_*_ADDRESS" signifie une notification ADDITIONAL_IP4_ADDRESS ou ADDITIONAL_IP6_ADDRESS.

```
    Initiateur                                          Répondant
HDR, SK { IDi, [CERT], [IDr], AUTH,
          [CP(CFG_REQUEST)] SAi2, TSi, TSr,
          N(MOBIKE_SUPPORTED),
          [N(ADDITIONAL_*_ADDRESS)+] }  -->

                                          <--  HDR, SK { IDr, [CERT], AUTH,
                                                 [CP(CFG_REPLY)], SAr2, TSi, TSr,
                                                 N(MOBIKE_SUPPORTED)
                                                 [N(ADDITIONAL_*_ADDRESS)+] }
```

Le receveur mémorise ces informations, mais aucune autre action n'est effectuée pour l'instant.

Bien que l'initiateur et le répondant tiennent tous deux un ensemble d'adresses d'homologues (logiquement associées à la IKE_SA) il est important de noter qu'ils utilisent ces informations pour des objets légèrement différents.

L'initiateur utilise l'ensemble d'adresses du répondant comme entrées à sa politique de choix d'adresse ; il peut, à un moment ultérieur, décider de déplacer le trafic IPsec sur une de ces adresses en utilisant la procédure décrite au paragraphe 3.5. Le répondant n'utilise normalement pas l'ensemble d'adresses de l'initiateur : les adresses sont utilisées seulement quand la propre adresse du répondant change (voir au paragraphe 3.6).

L'ensemble des adresses disponibles aux homologues peut changer pendant la durée de vie de la IKE_SA. La procédure pour mettre à jour ces informations est décrite au paragraphe 3.6.

Noter que si des interfaces de l'initiateur sont derrière un NAT (du point de vue du répondant) les adresses reçues par le répondant vont être incorrectes. Cela signifie que la procédure pour changer les adresses du répondant décrite au paragraphe 3.6 ne fonctionne pas complètement quand l'initiateur est derrière un NAT. Pour la même raison, les homologues NE DEVRAIENT PAS aussi utiliser ces informations pour autre chose que ce qui est explicitement décrit dans le présent document ou une future spécification qui le mettrait à jour.

3.5 Changement des adresses dans les SA IPsec

Dans MOBIKE, l'initiateur décide quelles adresses sont utilisées dans les SA IPsec. C'est-à-dire que le répondant ne met normalement pas à jour de SA IPsec sans avoir reçu une demande explicite UPDATE_SA_ADDRESSES de l'initiateur. (Comme décrit ci-dessous, le répondant peut cependant mettre à jour la IKE_SA dans certaines circonstances.)

Les raisons pour lesquelles l'initiateur souhaite changer les adresses sortent largement du domaine d'application de MOBIKE. Normalement, le déclenchement inclut des informations reçues des couches inférieures, comme des changements des adresses IP ou des indications de liaison morte. Certaines de ces informations peuvent être non fiables : par exemple, des messages ICMP pourraient être falsifiés par un attaquant. Des informations non fiables DEVRAIENT n'être traitées que comme une indication qu'il pourrait y avoir un problème, et l'initiateur DEVRAIT déclencher la détection d'homologue mort (DPD, *Dead Peer Detection*) (c'est à dire, envoyer une demande INFORMATIONAL) pour déterminer si le chemin actuel est toujours utilisable.

Le changement d'adresses peut aussi être déclenché par des événements dans IKEv2. Au moins les évenements suivants

peuvent être cause que l'initiateur réévalue sa politique locale de choix d'adresse, conduisant éventuellement à changer les adresses.

- Une demande IKEv2 a été retransmise plusieurs fois, mais aucune réponse valide n'a été reçue. Cela suggère que le chemin actuel n'est plus en fonctionnement.

- Une demande INFORMATIONAL contenant une notification ADDITIONAL_IP4_ADDRESS, ADDITIONAL_IP6_ADDRESS, ou NO_ADDITIONAL_ADDRESSES est reçue. Cela signifie que les adresses de l'homologue pourraient avoir changé. Ceci est particulièrement important si l'ensemble annoncé d'adresses ne contient plus l'adresse actuellement utilisée.

- Une notification UNACCEPTABLE_ADDRESSES est reçue en réponse à une demande de mise à jour d'adresse (décrite plus loin).

- L'initiateur reçoit une notification NAT_DETECTION_DESTINATION_IP qui ne correspond pas à la précédente réponse UPDATE_SA_ADDRESSES (voir au paragraphe 3.8 une description plus détaillée).

La description dans la suite de ce paragraphe suppose que l'initiateur a déjà décidé ce que devraient être les nouvelles adresses. Quand cette décision a été prise, l'initiateur :

- Met à jour la IKE_SA avec les nouvelles adresses, et établit le fanion "mise à jour en cours" dans la IKE_SA.

- Met à jour les SA IPsec associées à cette IKE_SA avec les nouvelles adresses (sauf si la politique de l'initiateur exige une vérification de l'acheminement de retour avant de mettre à jour les SA IPsec, et si la vérification n'a pas déjà été faite pour cette adresse du répondant).

- Si les SA IPsec ont été mises à jour dans l'étape précédente : si la traversée de NAT n'est pas activée, et si le répondant prend en charge la traversée de NAT (comme indiqué par les charges utiles détection de NAT dans l'échange IKE_SA_INIT) et si l'initiateur suspecte ou sait qu'un NAT est probablement présent, il active la traversée de NAT (c'est-à-dire, il active l'encapsulation UDP des paquets ESP sortants et il envoie des paquets de NAT-Keepalive).

- Si il y a des demandes IKEv2 en cours (demandes pour lesquelles l'initiateur n'a pas encore reçu de réponse) il continue de les retransmettre en utilisant les adresses dans la IKE_SA (les nouvelles adresses).

- Quand la taille de fenêtre le permet, il envoie une demande INFORMATIONAL contenant la notification UPDATE_SA_ADDRESSES (qui ne contient aucune donnée) et met à zéro le fanion "mise à jour en cours". La demande va être comme suit :

Initiateur **Répondant**

```
HDR, SK { N(UPDATE_SA_ADDRESSES),
          [N(NAT_DETECTION_SOURCE_IP),
           N(NAT_DETECTION_DESTINATION_IP)],
          [N(NO_NATS_ALLOWED)], [N(COOKIE2)] } ------->
```

- Si un nouveau changement d'adresse survient pendant l'attente de la réponse, recommencer à partir de la première étape (et ignorer les réponses à cette demande UPDATE_SA_ADDRESSES).

Quand il traite une demande INFORMATIONAL contenant la notification UPDATE_SA_ADDRESSES, le répondant :

- Détermine si il a déjà reçu une demande UPDATE_SA_ADDRESSES plus récente que celle là (si le répondant utilise une taille de fenêtre supérieure à un, il est possible que des demandes soient reçue déclassées). Si c'est le cas, un message de réponse normal (décrit plus loin) est envoyé, mais aucune autre action n'est effectuée.

- Si la notification NO_NATS_ALLOWED est présente, la traiter comme décrit au paragraphe 3.9.

- Vérifier que la paire (adresse IP de source, adresse IP de destination) dans l'en-tête IP est acceptable en accord avec la politique locale. Si elle ne l'est pas, répondre par un message contenant la notification UNACCEPTABLE_ADDRESSES (et éventuellement COOKIE2).

- Met à jour les adresses IP dans la IKE_SA avec les valeurs provenant de l'en-tête IP. (Utiliser l'adresse provenant de l'en-tête IP est cohérent avec le IKEv2 normal, et permet à IKEv2 de travailler avec des NAT sans qu'il soit besoin

d'une auto réparation unilatérale d'adresse [RFC3424].)

o Réplique par une réponse INFORMATIONAL :

Initiateur	**Répondant**
	HDR, SK { [N(NAT_DETECTION_SOURCE_IP), N(NAT_DETECTION_DESTINATION_IP)], [N(COOKIE2)] }

o Nécessairement, initie une vérification d'acheminement de retour pour la nouvelle adresse de l'initiateur (voir le paragraphe 3.7) et attend la fin de la vérification.

o Met à jour les SA IPsec associées à cette IKE_SA avec les nouvelles adresses.

o Si traversée de NAT est prise en charge et que des charges utiles Détection de NAT étaient incluses, activer ou désactiver la traversée de NAT.

Quand l'initiateur reçoit la réponse :

o Si un changement d'adresse s'est produit après l'envoi de la première demande, aucun traitement MOBIKE n'est fait pour le message de réponse parce que une nouvelle UPDATE_SA_ADDRESSES est en train d'être envoyée (ou a déjà été envoyée, si la taille de fenêtre supérieure à un est utilisée).

o Si la réponse contient la notification UNEXPECTED_NAT_DETECTED, l'initiateur traite la réponse comme décrit au paragraphe 3.9.

o Si la réponse contient une notification UNACCEPTABLE_ADDRESSES, l'initiateur PEUT choisir une autre adresse et réessayer l'échange, continuer en utilisant les adresses précédemment utilisées, ou déconnecter.

o Il met à jour les SA IPsec associées à cette IKE_SA avec les nouvelles adresses (sauf si cela a déjà été fait précédemment avant d'envoyer la demande ; c'est le cas quand aucune vérification de l'acheminement de retour n'a été exigée).

o La traversée de NAT est prise en charge et des charges utiles Détection de NAT ont été incluses, l'initiateur active ou désactive la traversée de NAT.

Il y a une exception à la règle que le répondant ne met jamais à jour de SA IPsec sans avoir reçu une demande UPDATE_SA_ADDRESSES. Si l'adresse de source que le répondant utilise actuellement devient indisponible (c'est-à-dire, l'envoi de paquets qui utilisent cette adresse de source n'est plus possible) il est permis au répondant de mettre à jour les SA IPsec pour utiliser une autre adresse (en plus d'initier la procédure décrite au prochain paragraphe).

3.6 Mise à jour des adresses supplémentaires

Comme décrit au paragraphe 3.4, l'initiateur et le répondant peuvent tous deux envoyer une liste d'adresses supplémentaires dans l'échange IKE_AUTH. Ces informations peuvent être mises à jour en envoyant un message de demande d'échange INFORMATIONAL qui contient une ou plusieurs notifications ADDITIONAL_IP4_ADDRESS/ ADDITIONAL_IP6_ADDRESS ou la notification NO_ADDITIONAL_ADDRESSES.

Si l'initiateur de l'échange a seulement une adresse IP, elle est placée dans l'en-tête IP, et le message contient la notification NO_ADDITIONAL_ADDRESSES. Si l'initiateur de l'échange a plusieurs adresses, une d'elles est placée dans l'en-tête IP, et le reste dans les notifications ADDITIONAL_IP4_ADDRESS/ADDITIONAL_IP6_ADDRESS.
La nouvelle liste d'adresses remplace les vieilles informations (en d'autres termes, ce ne sont pas des opérations ajout/supression séparées ; la liste complète est envoyée chaque fois que ces notifications sont utilisées).

L'échange de messages va ressembler à ceci :

Initiateur	**Répondant**
HDR, SK { [N(ADDITIONAL_*_ADDRESS)+], [N(NO_ADDITIONAL_ADDRESSES)], [N(NO_NATS_ALLOWED)], [N(COOKIE2)] } ---------->	
	<--------- HDR, SK { [N(COOKIE2)] }

Quand une demande contenant une notification ADDITIONAL_IP4_ADDRESS, ADDITIONAL_IP6_ADDRESS, ou quand une notification NO_ADDITIONAL_ADDRESSES est reçue, le répondant à l'échange :

- Détermine si il a déjà reçu une demande plus récente de mise à jour des adresses (si une taille de fenêtre supérieure à un est utilisée, il est possible que les demandes ne soient pas reçues dans l'ordre). Si c'est le cas, un message de réponse est envoyé, mais l'ensemble d'adresses n'est pas mis à jour.

- Si la notification NO_NATS_ALLOWED est présente, il la traite comme décrit au paragraphe 3.9.

- Met à jour l'ensemble d'adresses de l'homologue sur la base de l'en-tête IP et des notifications ADDITIONAL_IP4_ADDRESS, ADDITIONAL_IP6_ADDRESS, et NO_ADDITIONAL_ADDRESSES.

- Envoie une réponse.

L'initiateur PEUT inclure ces notifications dans la même demande que UPDATE_SA_ADDRESSES.

Si la demande de mise à jour des adresses est retransmiqe en utilisant plusieurs adresses de source différentes, une nouvelle demande INFORMATIONAL DOIT être envoyée.

Il y a une complication supplémentaire : quand le répondant veut mettre à jour le jeu d'adresses, les adresses actuellement utilisées peuvent ne plus fonctionner. Dans ce cas, le répondant utilise la liste des adresses supplémentaires reçue de l'initiateur, et la liste de ses propres adresses, pour déterminer quelles adresses utiliser pour envoyer la demande INFORMATIONAL. C'est la seule fois où le répondant utilise la liste des adresses supplémentaires reçue de l'initiateur.

Noter que les deux homologues peuvent avoir leur propre politique sur quelles adresses sont d'utilisation acceptable, et certains types de politiques peuvent simplifier la mise en œuvre. Par exemple, si le répondant a une seule adresse fixée, il n'a pas besoin de traiter les notifications ADDITIONAL_IP4_ADDRESS et ADDITIONAL_IP6_ADDRESS qu'il reçoit (au delà d'ignorer les notifications d'état non reconnues, comme déjà exigé dans la [RFC4306]). De plus, si l'initiateur a une politique qui dit que seule l'adresse de répondant spécifiée dans la configuration locale est acceptable, il n'a pas à envoyer ses propres adresses supplémentaires au répondant (car le répondant n'a pas besoin d'elles sauf quand il change sa propre adresse).

3.7 Vérification de l'acheminement de retour

Les deux parties peuvent facultativement vérifier que l'autre partie peut bien recevoir les paquets à l'adresse revendiquée. Par défaut, cette "vérification de l'acheminement de retour" DEVRAIT être effectuée. Dans des environnements où l'homologue est supposé bien se comporter (par exemple dans de nombreux VPN d'entreprise) ou où l'adresse peut être vérifiée par d'autres moyens (par exemple, un certificat produit par une autorité de confiance pour cet objet) la vérification d'acheminement de retour PEUT être omise.

La vérification peut être effectuée avant la mise à jour des SA IPsec, immédiatement après leur mise à jour, ou de façon continue durant la connexion. Par défaut, la vérification d'acheminement de retour DEVRAIT être faite avant de mettre à jour les SA IPsec, mais dans certains environnements elle PEUT être retardée jusque après la mise à jour des SA IPsec.

Tout échange INFORMATIONAL peut être utilisé pour les besoins de la vérification d'acheminement de retour, à une exception près (décrite plus loin) : quand une réponse valide est reçue, on sait que l'autre partie peut recevoir les paquets à l'adresse revendiquée.

Pour s'assurer que l'homologue ne peut pas générer la réponse INFORMATIONAL correcte sans avoir vu la demande, une nouvelle charge utile est ajoutée aux messages INFORMATIONAL. L'envoyeur d'une demande INFORMATIONAL PEUT inclure une notification COOKIE2, et si elle est incluse, le receveur d'une demande INFORMATIONAL DOIT copier la notification telle qu'elle dans la réponse. Quand il traite la réponse, l'envoyeur d'origine DOIT vérifier que la valeur est la même que celle envoyée. Si les valeurs ne correspondent pas, la IKE_SA DOIT être close. (Voir aussi le paragraphe 4.2.5 pour le format de la notification COOKIE2.)

L'exception mentionnée plus haut est la suivante : si la même demande INFORMATIONAL a été envoyée à plusieurs adresses différentes (c'est-à-dire, si l'adresse de destination dans la IKE_SA a été mise à jour après que la demande a été envoyée) la réception de la réponse INFORMATIONAL ne dit pas quelle adresse est celle qui fonctionne. Dans ce cas, une nouvelle demande INFORMATIONAL doit être envoyée pour vérifier l'acheminement de retour.

3.8 Changements des transpositions de NAT

IKEv2 effectue la détection d'homologue mort (DPD, *Dead Peer Detection*) si il y a eu récemment seulement du trafic sortant sur toutes les SA associées à la IKE_SA.

Dans MOBIKE, ces messages peuvent aussi être utilisés pour détecter si des transpositions de NAT ont changé (par exemple, si l'intervalle de garde en vie est trop long, ou si le boîtier de NAT est réamorcé). Plus précisément, si les deux homologues prennent tous deux en charge la présente spécification et la traversée de NAT, les notifications NAT_DETECTION_SOURCE_IP et NAT_DETECTION_DESTINATION_IP PEUVENT être incluses dans toute demande INFORMATIONAL ; si la demande les inclut, le répondant DOIT aussi les inclure dans la réponse (mais aucune autre action est effectuée, sauf spécification contraire).

Quand l'initiateur est derrière un NAT (comme détecté plus tôt en utilisant les notifications NAT_DETECTION_SOURCE_IP et NAT_DETECTION_DESTINATION_IP) il DEVRAIT inclure ces notifications dans les messages de DPD et comparer les notifications NAT_DETECTION_DESTINATION_IP reçues avec la valeur de la réponse UPDATE_SA_ADDRESSES précédente (ou la réponse IKE_SA_INIT). Si les valeurs ne correspondent pas, l'adresse IP et/ou l'accès vus par le répondant ont changé, et l'initiateur DEVRAIT envoyer un UPDATE_SA_ADDRESSES comme décrit au paragraphe 3.5. Si l'initiateur suspecte que la transposition de NAT a changé, il PEUT aussi sauter l'étape de détection et envoyer immédiatement le UPDATE_SA_ADDRESSES. Cela économise un aller-retour si la transposition de NAT a bien changé.

Noter que cette approche de la détection des changements de transposition de NAT peut causer une mise à jour d'adresse supplémentaire quand les clés de la SA IKE sont changées. C'est parce que le hachage de NAT_DETECTION_DESTINATION_IP inclut aussi les indices de paramètre de sécurité (SPI, *Security Parameter Index*) IKE, qui changent quand on effectue un changement de clés. Cette mise à jour inutile est cependant sans danger.

Quand MOBIKE est utilisé, les mises à jour dynamiques (spécifiées dans la [RFC4306], paragraphe 2.23) où l'adresse et l'accès de l'homologue sont mis à jour à partir du dernier paquet valide authentifié, fonctionnent d'une façon légèrement différente. L'hôte qui n'est pas derrière un NAT NE DOIT PAS utiliser ces mises à jour dynamiques pour les paquets IKEv2, mais PEUT les utiliser pour les paquets ESP. Cela assure qu'un échange INFORMATIONAL qui ne contient pas de UPDATE_SA_ADDRESSES ne cause aucun changement, lui permettant d'être utilisé pour, par exemple, vérifier si un chemin particulier fonctionne.

3.9 Interdiction de NAT

La prise en charge de IKEv2/IPsec de base sans traversée de NAT peut fonctionner sur certains types de NAT de un à un "de base" et d'agents de traduction IPv4/IPv6 en mode tunnel. C'est parce que la somme de contrôle d'intégrité IKEv2 ne couvre pas les adresses dans l'en-tête IP. Cela peut être considéré comme posant problème dans certaines circonstances, parce que en un certain sens toute modification des adresses IP peut être considérée comme une attaque.

La présente spécification traite ce problème en protégeant les adresses IP quand la traversée de NAT n'a pas été explicitement activée. Cela signifie que MOBIKE sans prise en charge de la traversée de NAT ne va pas fonctionner si les chemins contiennent des NAT, des agents de traduction IPv4/IPv6, ou d'autres nœuds qui modifient les adresses dans l'en-tête IP. Cette caractéristique est principalement destinée aux cas de IPv6 et de VPN de site à site, où les administrateurs peuvent savoir à l'avance qu'il n'y a pas de NAT, et donc que toute modification au paquet peut être considérée comme une attaque.

Plus précisément, quand la traversée de NAT n'est pas activée, tous les messages qui peuvent mettre à jour les adresses associées à la IKE_SA et/ou aux SA IPsec (la première demande IKE_AUTH et toutes les demandes INFORMATIONAL qui contiennent une des notifications suivantes : UPDATE_SA_ADDRESSES, ADDITIONAL_IP4_ADDRESS, ADDITIONAL_IP6_ADDRESS, NO_ADDITIONAL_ADDRESSES) DOIVENT aussi inclure une notification NO_NATS_ALLOWED. Le répondant à l'échange DOIT vérifier que le contenu de la notification NO_NATS_ALLOWED correspond aux adresses dans l'en-tête IP. Si elles ne correspondent pas, une réponse contenant une notification UNEXPECTED_NAT_DETECTED est envoyée. Le message de réponse est envoyé à l'adresse et accès d'où la demande correspondante venait, non à l'adresse contenue dans la notification NO_NATS_ALLOWED.

Si l'initiateur de l'échange reçoit une notification UNEXPECTED_NAT_DETECTED en réponse à sa demande INFORMATIONAL, il DEVRAIT reessayer l'opération plusieurs fois en utilisant de nouvelles demandes

INFORMATIONAL. De même, si l'initiateur reçoit UNEXPECTED_NAT_DETECTED dans l'échange IKE_AUTH, il DEVRAIT reessayer plusieurs fois l'établissement de la SA IKE en commençant par une nouvelle demande IKE_SA_INIT. Cela assure qu'un attaquant capable de modifier seulement un paquet ne cause pas inutilement l'inutilisation d'un chemin. Le nombre exact d'essais n'est pas spécifié dans le présent document parce que cela n'affecte pas l'interopérabilité. Cependant, parce que le message IKE va aussi être rejeté si l'attaquant modifie le champ de somme de contrôle d'intégrité, un nombre raisonnable pourrait être ici le nombre de reessais qui est utilisé pour les retransmissions normales.

Si une notification UNEXPECTED_NAT_DETECTED est envoyée, le répondant à l'échange NE DOIT PAS utiliser le contenu de la notification NO_NATS_ALLOWED pour un autre objet qu'éventuellement enregistrer les informations dans un but de réparation.

3.10 Vérifications de chemin

La détection d'homologue mort de IKEv2 permet aux homologues de détecter si le chemin actuellement utilisé a cessé de fonctionner. Cependant, si l'un ou l'autre des homologues a plusieurs adresses, la détection d'homologue mort seule ne dit pas lequel des autres chemins pourrait fonctionner.

Si c'est exigé par sa politique de choix d'adresse, l'initiateur peut utiliser les messages normaux de demande/réponse IKEv2 INFORMATIONAL pour vérifier si un certain chemin fonctionne. Les mises en œuvre PEUVENT vérifier le chemin même si le chemin actuellement utilisé fonctionne pour, par exemple, détecter quand un meilleur chemin (précédemment indisponible) devient disponible.

3.11 Échec de récupération et fins de temporisation

Dans MOBIKE, l'initiateur est chargé de détecter et récupérer de la plupart des défaillances.

Pour donner à l'initiateur assez de temps pour détecter l'erreur, le répondant DEVRAIT utiliser des intervalles de temporisation relativement longs quand, par exemple, il retransmet des demandes IKEv2 ou qu'il décide si il va initier la détection d'homologue mort. Bien qu'il ne soit pas exigé de longueurs spécifiques de temporisation, il est suggéré que les répondants continuent de retransmettre les demandes IKEv2 pendant au moins cinq minutes avant d'abandonner.

3.12 Détection d'homologue mort

MOBIKE utilise la même méthode de détection d'homologue mort que l'IKEv2 normal, mais comme les adresses peuvent changer, il n'est pas suffisant de juste vérifier que l'homologue est en vie, mais aussi qu'il est synchronisé avec les mises à jour d'adresse et n'a pas, par exemple, ignoré une mise à jour d'adresse à cause d'un échec d'exécution de l'essai d'acheminement de retour. Cela signifie que quand il y a des paquets IPsec entrants, les nœuds MOBIKE DEVRAIENT inspecter les adresses utilisées dans ces paquets et vérifier qu'elles correspondent à celles qui devraient être employées. Si elles ne correspondent pas, de tels paquets NE DEVRAIENT PAS être utilisés comme preuve que l'homologue est capable de communiquer avec ce nœud et/ou que l'homologue a reçu toutes les mises à jour d'adresses.

4. Formats de charge utile

La présente spécification définit plusieurs nouveaux types de charge utile Notify IKEv2. Voir au paragraphe 3.10 de la [RFC4306] une description générale de la charge utile Notify.

4.1 Messages Notify – types d'erreur

4.1.1 Charge utile Notify ADRESSES_INACCEPTABLES

Le répondant peut inclure cette notification dans une réponse d'échange INFORMATIONAL pour indiquer que le changement d'adresse dans le message de demande correspondant (qui contenait une notification UPDATE_SA_ADDRESSES) n'a pas été effectué.

Le type de message Notify pour UNACCEPTABLE_ADDRESSES est 40. Les champs Identifiant de protocole et Taille de SPI sont réglés à zéro. Il n'y a pas de données associées à ce type Notify.

4.1.2 Charge utile Notify NAT_INATTENDU_DÉTECTÉ

Voir la description de cette notification au paragraphe 3.9.

Le type de message Notify pour UNEXPECTED_NAT_DETECTED est 41. Les champs Identifiant de protocole et Taille de SPI sont réglés à zéro. Il n'y a pas de données associées à ce type Notify.

4.2 Messages Notify – types d'état

4.2.1 Charge utile Notify MOBIKE_PRIS_EN_CHARGE

La notification MOBIKE_SUPPORTED est incluse dans l'échange IKE_AUTH pour indiquer que la mise en œuvre prend en charge la présente spécification.

Le type de message Notify pour MOBIKE_SUPPORTED est 16396. Les champs Identifiant de protocole et Taille de SPI sont réglés à zéro. Le champ Données de notification DOIT être laissé vide (longueur zéro) à l'envoi, et son contenu (si il en est) DOIT être ignoré quand cette notification est reçue. Cela permettra que le champ soit utilisé par de futures versions de ce protocole.

4.2.2 Charges utiles Notify ADRESSE_IP4_SUPPLÉMENTAIRE et ADRESSE_IP6_SUPPLÉMENTAIRE

Les deux parties peuvent inclure des notifications ADDITIONAL_IP4_ADDRESS et/ou ADDITIONAL_IP6_ADDRESS dans l'échange IKE_AUTH et dans les messages de demande d'échange INFORMATIONAL ; voir une description plus détaillée aux paragraphes 3.4 et 3.6.

Les types de message Notify pour ADDITIONAL_IP4_ADDRESS et ADDITIONAL_IP6_ADDRESS sont respectivement 16397 et 16398. Les champs Identifiant de protocole et Taille de SPI sont réglés à zéro. Les données associées à ces types Notify sont soit une adresse IPv4 de quatre octets, soit une adresse IPv6 de seize octets.

4.2.3 Charge utile Notify PAS_D'ADRESSES_SUPPLÉMENTAIRES

La notification NO_ADDITIONAL_ADDRESSES peut être incluse dans un message de demande d'échange INFORMATIONAL pour indiquer que l'initiateur de l'échange n'a pas d'autre adresse que celle utilisée dans l'échange (voir une description plus détaillée au paragraphe 3.6).

Le type de message Notify pour NO_ADDITIONAL_ADDRESSES est 16399. Les champs Identifiant de protocole et Taille de SPI sont réglés à zéro. Il n'y a pas de données associées à ce type Notify.

4.2.4 Charge utile Notify MISE_À_JOUR_DES_ADRESSES_DE_SA

Cette notification est incluse dans les demandes d'échange INFORMATIONAL envoyées par l'initiateur pour mettre à jour les adresses des SA IKE_SA et IPsec (voir le paragraphe 3.5).

Le type de message Notify pour UPDATE_SA_ADDRESSES est 16400. Les champs Identifiant de protocole et Taille de SPI sont réglés à zéro. Il n'y a pas de données associées à ce type Notify.

4.2.5 Charge utile Notify COOKIE2

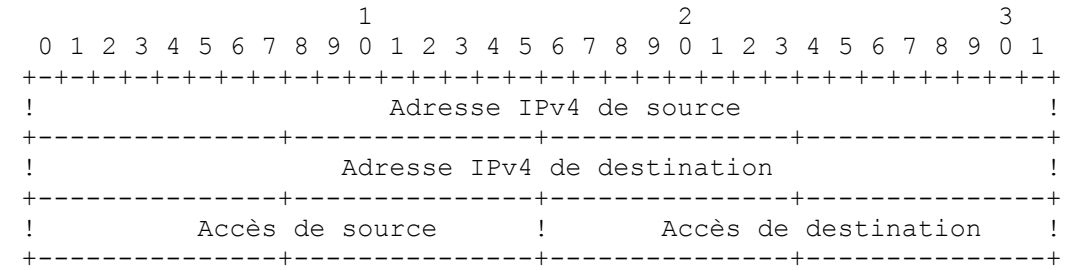
Cette notification PEUT être incluse dans toute demande INFORMATIONAL pour les besoins de la vérification de l'acheminement de retour (voir le paragraphe 3.7). Si la demande INFORMATIONAL inclut COOKIE2, le répondant à l'échange DOIT copier la notification dans le message de réponse.

Les données associées à cette notification DOIVENT faire entre 8 et 64 octets (inclus) et DOIVENT être choisies par l'initiateur de l'échange d'une façon imprévisible pour le répondant à l'échange. Le type de message Notify pour ce message est 16401. Les champs Identifiant de protocole et Taille de SPI sont réglés à zéro.

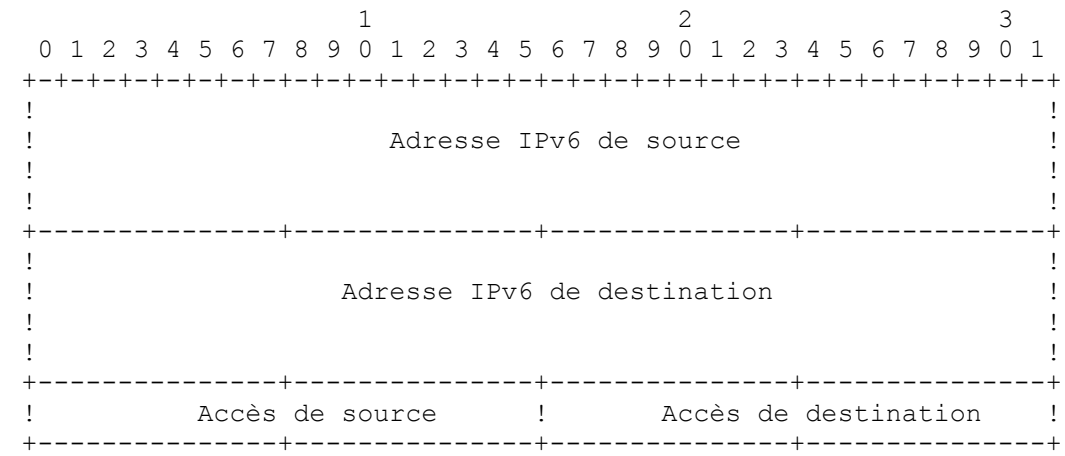
4.2.6 Charge utile Notify PAS_DE_NAT_PERMIS

Voir la description de cette notification au paragraphe 3.9.

Le type de message Notify pour ce message est 16402. Les données de notification contiennent les adresses IP et accès d'où et à qui le paquet a été envoyé. Pour IPv4, les données de notification sont de 12 octets et sont définies comme suit :



Pour IPv6, les données de notification sont de 36 octets et sont définies comme suit :



Les champs Identifiant de protocole et Taille de SPI sont réglés à zéro.

5. Considérations sur la sécurité

Les buts pricipaux de la présente spécification sont de maintenir la sécurité offerte par les procédures usuelles de IKEv2 et de contrer les menaces relatives à la mobilité de façon appropriée. Cette Section décrit les nouvelles considérations de sécurité introduites par MOBIKE. Voir dans la [RFC4306] les considérations générales pour la sécurité dans IKEv2.

5.1 Redirection et capture du trafic

Les charges utiles MOBIKE relatives à la mise à jour des adresses sont chiffrées, protégées en intégrité et contre la répétition en utilisant la SA IKE. Cela assure que personne excepté les participants ne peut, par exemple, faire qu'un message de commande change les adresses.

Cependant, comme avec le IKEv2 normal, les adresses IP réelles dans l'en-tête IP ne sont pas couvertes par la protection de l'intégrité. Cela signifie qu'un NAT entre les parties (ou un attaquant agissant comme un NAT) peut modifier les adresses et causer l'utilisation d'adresses IP d'en-tête de tunnel (externe) incorrectes pour les SA IPsec. La portée de cette attaque est limitée principalement au déni de service parce que tout le trafic est protégé en utilisant IPsec.

Cette attaque peut seulement être lancée par des attaquants sur le chemin qui sont capables de modifier les messages IKEv2 portant des charges utiles de détection de NAT (comme les messages de détection d'homologue mort). En modifiant l'en-tête IP de ces paquets, les attaquants peuvent conduire les homologues à croire qu'il existe un nouveau NAT ou un lien de NAT changé entre eux. L'attaque peut continuer tant que l'attaquant est sur le chemin, en modifiant les messages IKEv2. Si ce n'est plus le cas, les mécanismes IKEv2 et MOBIKE conçus pour détecter les changements de transposition de NAT

vont finalement reconnaître que le trafic prévu ne passe plus, et vont mettre à jour les adresses de façon appropriée.

MOBIKE introduit la notification NO_NATS_ALLOWED qui est utilisée pour détecter la modification, par des extérieurs, des adresses dans l'en-tête IP. Quand cette notification est utilisée, la communication à travers les NAT et autres traducteurs d'adresses est impossible, de sorte qu'elle n'est envoyée que quand il n'y a pas de traversée de NAT. Cette caractéristique est principalement destinée à IPv6 et aux cas de VPN de site à site, où les administrateurs peuvent savoir à l'avance qu'il n'y a pas de NAT présent.

5.2 Protection de la charge utile IPsec

L'utilisation de la protection de IPsec sur le trafic de charges utiles protège les participants contre la divulgation du contenu du trafic, si le trafic devait finir sur une destination incorrecte ou être soumis à l'espionnage.

Cependant, les associations de sécurité créées à l'origine pour la protection d'un flux spécifique entre des adresses spécifiques peuvent être mises à jour ultérieurement par MOBIKE. Ceci doit être pris en compte si l'adresse IP (externe) de l'homologue a été utilisée quand on décide quelle sorte de SA IPsec l'homologue est autorisé à créer.

Par exemple, le niveau de protection requis peut dépendre de la localisation actuelle du VPN client, ou l'accès peut être permis seulement à partir de certaines adresses IP.

Il est recommandé que les politiques de sécurité, pour les homologues qui sont autorisés à utiliser MOBIKE, soient configurées d'une manière qui prend en compte qu'une seule association de sécurité peut être utilisée à des moments différents à travers des chemins qui ont des propriétés de sécurité diverses.

Ceci est particulièrement critique pour l'autorisation de sélecteur de trafic. La base de données (logique) d'autorisation d'homologues (PAD, *Peer Authorization Database*) contient les informations utilisées par IKEv2 quand il détermine quelles sortes de SA IPsec un homologue est autorisé à créer. Ce processus est décrit au paragraphe 4.4.3 de la [RFC4301]. Quand un homologue demande la création d'une SA IPsec avec certains sélecteurs de trafic, la PAD doit contenir des "données d'autorisation de SA fille" reliant l'identité authentifiée par IKEv2 et les adresses permises pour les sélecteurs de trafic. Voir aussi dans la [RFC4718] une discussion plus développée.

Il est important de noter qu'envoyer simplement des paquets IKEv2 en utilisant une adresse particulière n'implique pas automatiquement une permission de créer des SA IPsec avec cette adresse dans les sélecteurs de trafic. Cependant, certaines mises en œuvre sont connues pour utiliser des politiques où être simplement accessible à une certaine adresse X implique une permission temporaire de créer des SA IPsec pour l'adresse X. Ici, "être accessible" signifie généralement la capacité d'envoyer (ou de simuler) des paquets IP avec l'adresse de source X et recevoir(ou espionner) les paquets envoyés à X.

Utiliser cette sorte de politiques ou extensions avec MOBIKE peut demander une attention particulière pour appliquer la nature temporaire de la permission. Par exemple, quand l'homologue passe à une autre adresse Y (et n'est plus accessible à X) il peut être nécessaire de clore les SA IPsec avec des sélecteurs de trafic correspondant à X. Cependant, ces interactions sortent du domaine d'application du présent document.

5.3 Attaques de déni de service contre des tiers

La redirection du trafic peut ne pas être effectuée juste pour obtenir l'accès au trafic ou pour dénier le service aux homologues, mais aussi pour causer une attaque de déni de service chez un tiers. Par exemple, une session TCP à haut débit, ou un flux multimédia, peut être redirigé sur un hôte victime, causant des dommages à ses capacités de communication.

Les attaquants dans cette menace peuvent être des extrérieurs ou même un des homologues IKEv2. Dans les scénarios usuels d'usage de VPN, les attaques par les homologues peuvent être facilement traitées si l'authentification effectuée dans la négociation initiale IKEv2 peut être retracée aux personnes qui peuvent être tenues pour responsables de l'attaque. Ce peut n'être pas le cas dans tous les scénarios, particulièrement avec des approches opportunistes de la sécurité.

Si l'attaque est lancée par un extérieur, le flux de trafic va normalement s'arrêter rapidement à cause du manque de réponses (comme des accusés de réception de couche transport). Cependant, si le receveur original du flux est malveillant, il pourrait maintenir le flux de trafic pendant une longue période, car il sera souvent capable d'envoyer les accusés de réception requis (voir dans [Aura02] une discussion plus étendue).

On devrait aussi noter, comme montré dans [Bombing], que sans filtrage d'entrée dans le réseau de l'attaquant, de telles attaques sont déjà possibles simplement en envoyant directement des paquets falsifiés de l'attaquant à la victime. De plus, si le réseau de l'attaquant a un filtrage d'entrée, cette attaque est aussi largement prévenue pour MOBIKE. Par conséquent, il y a peu de sens à se protéger contre des attaques de nature similaire dans MOBIKE. Cependant, il y a du sens à limiter les capacités d'amplification fournies aux attaquants, afin qu'ils ne puissent pas utiliser la redirection de flux pour envoyer un grand nombre de paquets à la victime en envoyant juste quelques paquets eux-mêmes.

La présente spécification inclut des vérifications d'acheminement de retour pour limiter la durée de toute attaque de "bombardement de tiers" par des attaquants hors chemin (par rapport à la victime). Les vérifications sont des messages authentifiés auxquels l'homologue doit répondre, et peuvent être effectuées avant que le changement d'adresse prenne effet, immédiatement après, ou même périodiquement durant la session. Les vérifications contiennent des données imprévisibles, et seulement quelques unes qui ont les clés associées à la SA IKE et ont vu le paquet de demande peuvent répondre correctement à la vérification.

La durée de l'attaque peut aussi être limitée si la victime rapporte le trafic non désiré au point d'extrémité du tunnel IPsec générateur en utilisant des messages d'erreur ICMP ou des notifications INVALID_SPI. Comme décrit au paragraphe 2.21 de la [RFC4306], ceci DEVRAIT déclencher une vérification de vivacité, qui sert aussi de double à la vérification d'acheminement de retour si la notification COOKIE2 est incluse.

5.4 Contrefaçon des indications de connectivité réseau

Les attaquants peuvent falsifier diverses indications provenant des couches inférieures et du réseau pour tromper les homologues sur quelles adresses fonctionnent ou non. Par exemple, des attaquants peuvent falsifier des messages d'erreur de couche de liaison pour essayer de faire que les parties passent leur trafic ailleurs ou même déconnectent. Des attaquants peuvent aussi falsifier des informations relatives aux rattachements réseau, à la découverte de routeur, et aux allocations d'adresse pour essayer de faire croire aux parties qu'elles ont la connexité Internet quand, en réalité, elles ne l'ont pas.

Ceci peut causer l'utilisation d'adressese non préférées ou même un déni de service.

MOBIKE ne fournit de lui-même aucune protection pour les indications provenant d'autres parties de la pile de protocoles. Ces vulnérabilités peuvent être atténuées par l'utilisation de techniques spécifiques des autres parties de la pile, comme la validation des erreurs ICMP [RFC5927], la sécurité de la couche de liaison, ou l'utilisation de la [RFC3971] pour protéger la découverte de routeur IPv6 et de voisin.

Finalement, MOBIKE dépend de la livraison des messages IKEv2 pour déterminer quels chemins peuvent être utilisés. Si les messages IKEv2 envoyés en utilisant des adresses particulières de source et de destination atteignent le receveur et qu'une réponse est reçue, MOBIKE va généralement considérer que le chemin fonctionne ; si aucune réponse n'est reçue même après des retransmissions, MOBIKE va suspecter que le chemin est rompu. Un attaquant qui peut contrôler efficacement la livraison ou la non livraison des messages IKEv2 dans le réseau peut donc influencer quelles adresses sont réellement utilisées.

5.5 Divulgation d'adresse et de topologie

Les mises à jour d'adresses MOBIKE et les notifications ADDITIONAL_IP4_ADDRESS/ ADDITIONAL_IP6_ADDRESS révèlent des informations sur les réseaux auxquels les homologues sont connectés.

Par exemple, considérons un hôte A avec deux interfaces réseau : une connexion cellulaire et une connexion Ethernet filaire à un LAN d'entreprise. Si l'hôte A contacte l'hôte B en utilisant IKEv2 et envoie des notifications ADDITIONAL_IP4_ADDRESS/ADDITIONAL_IP6_ADDRESS, l'hôte B reçoit des informations supplémentaires qu'il pourrait ne pas connaître autrement. Si l'hôte A a utilisé la connexion cellulaire pour le trafic IKEv2, l'hôte B peut aussi voir l'adresse du LAN d'entreprise (et peut-être deviner de plus que l'hôte A est utilisé par un employé de cette entreprise). Si l'hôte A a utilisé le LAN d'entreprise pour faire la connexion, l'hôte B peut voir que l'hôte A a un abonnement chez cet opérateur cellulaire particulier.

Ces adresses supplémentaires peuvent aussi divulguer des informations de localisation plus précises que juste une seule adresse. Supposons que l'hôte A utilise sa connexion cellulaire pour le trafic IKEv2, mais envoie aussi une notification ADDITIONAL_IP4_ADDRESS contenant une adresse IP correspondant à un LAN sans fil d'un café particulier. Il est probable que l'hôte B peut maintenant mieux deviner la localisation de A qu'il n'aurait été possible sur la seule base de

l'adresse IP cellulaire.

De plus, comme décrit au paragraphe 3.4, certaines des adresses pourraient aussi être des adresses privées derrière un NAT.

Dans de nombreux environnements, divulguer des informations d'adresse n'est pas un problème (et bien sûr cela ne peut pas être évité si les hôtes souhaitent utiliser ces adresses pour le trafic IPsec). Par exemple, un client de VPN d'accès distant pourrait considérer la passerelle du VPN d'entreprise comme suffisamment digne de confiance pour ces besoins. De plus, les notifications ADDITIONAL_IP4_ADDRESS et ADDITIONAL_IP6_ADDRESS sont envoyées chiffrées, de sorte que les adresses ne sont pas visibles aux espions (sauf, bien sûr, si elles sont utilisées ensuite pour envoyer du trafic IKEv2/IPsec).

Cependant, si MOBIKE est utilisé dans une approche plus opportuniste, il peut être souhaitable de limiter les informations envoyées. Naturelement, les homologues n'ont pas à divulguer d'adresses qu'ils ne veulent pas utiliser pour le trafic IPsec. Aussi, comme noté au paragraphe 3.6, un initiateur dont la politique est de toujours utiliser l'adresse de répondant configurée en local n'a pas à envoyer de charges utiles ADDITIONAL_IP4_ADDRESS/ADDITIONAL_IP6_ADDRESS.

6. Considérations relatives à l'IANA

Le présent document ne crée aucun nouvel espace de noms à tenir par l'IANA, mais exige de nouvelles valeurs dans des espaces de noms qui ont été définis dans la spécification de base de IKEv2 [RFC4306].

Le présent document définit plusieurs nouvelles notifications IKEv2 dont les valeurs ont été allouées dans l'espace de noms "Types de message Notify IKEv2".

Messages Notify – types d'erreur	**Valeur**
UNACCEPTABLE_ADDRESSES	40
UNEXPECTED_NAT_DETECTED	41

Messages Notify – types d'état	**Valeur**
MOBIKE_SUPPORTED	16396
ADDITIONAL_IP4_ADDRESS	16397
ADDITIONAL_IP6_ADDRESS	16398
NO_ADDITIONAL_ADDRESSES	16399
UPDATE_SA_ADDRESSES	16400
COOKIE2	16401
NO_NATS_ALLOWED	16402

Ces notifications sont décrites à la Section 4.

7. Remerciements

Le présent document est l'effort collaboratif du groupe de travail MOBIKE tout entier. Des remerciements particuliers sont dus à Jari Arkko, Tuomas Aura, Marcelo Bagnulo, Stephane Beaulieu, Elwyn Davies, Lakshminath Dondeti, Francis Dupont, Paul Hoffman, James Kempf, Tero Kivinen, Pete McCann, Erik Nordmark, Mohan Parthasarathy, Pekka Savola, Bill Sommerfeld, Maureen Stillman, Shinta Sugimoto, Hannes Tschofenig, et Sam Vaarala. Le présent document incorpore aussi des idées et du texte des propositions antérieures de protocoles comme MOBIKE, incluant [AddrMgmt], [Kivinen], [MOPO], et [SMOBIKE], et le document de conception de MOBIKE [RFC4621].

8. Références

8.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

8.2 Références pour information

[AddrMgmt] Dupont, F., "Address Management for IKE version 2", Travail en cours, novembre 2005.

[Aura02] Aura, T., Roe, M., and J. Arkko, "Security of Internet Location Management", Proc. 18th Annual Computer Security Applications Conference (ACSAC), décembre 2002.

[Bombing] Dupont, F., "A note about 3rd party bombing in Mobile IPv6", Travail en cours, décembre 2005.

[DNA6] Narayanan, S., Daley, G., and N. Montavont, "Detecting Network Attachment in IPv6 - Best Current Practices for hosts", Travail en cours, octobre 2005.

[Kivinen] Kivinen, T., "MOBIKE protocol", Travail en cours, février 2004.

[MOPO] Eronen, P., "Mobility Protocol Options for IKEv2 (MOPO-IKE)", Travail en cours s, février 2005.

[RFC2461] T. Narten, E. Nordmark, W. Simpson, "Découverte de voisins pour IP version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4861) *(D.S.)*

[RFC3344] C. Perkins, éd., "Prise en charge de la mobilité IP pour IPv4", août 2002. (*Obsolète, voir* RFC5944) *(P.S.)*

[RFC3424] L. Daigle, éd., IAB, "Considérations de l'IAB sur l'auto correction d'adressage unilatérale (UNSAF) à travers la traduction d'adresse réseau", novembre 2002. *(Information)*

[RFC3489] J. Rosenberg et autres, "STUN - Simple traversée par le protocole de datagramme d'utilisateur (UDP) des traducteurs d'adresse réseau (NAT)", mars 2003. (*Obsolète, voir* RFC5389) *(P.S.)*

[RFC3775] D. Johnson, C. Perkins, J. Arkko, "Prise en charge de la mobilité dans IPv6", juin 2004. *(P.S.) (Obs., voir* RFC6275)

[RFC3971] J. Arkko et autres, "Découverte de voisin sûre (SEND)", mars 2005. (*MàJ par* RFC6494) *(P.S.)*

[RFC4436] B. Aboba et autres, "Détection des rattachements au réseau dans IPv4 (DNAv4)", mars 2006. *(P.S.)*

[RFC4621] T. Kivinen et autres, "Concept de protocole de mobilité et rattachement plusieurs IKEv2 (MOBIKE)", août 2006. *(Info.)*

[RFC4718] P. Eronen, P. Hoffman, "Précisions et lignes directrices pour la mise en œuvre de IKEv2", octobre 2006. *(Information)*

[RFC5927] F. Gont, "Attaques ICMP contre TCP", juillet 2010. *(Information)*

[SMOBIKE] Eronen, P. and H. Tschofenig, "Simple Mobility and Multihoming Extensions for IKEv2 (SMOBIKE)", Travail en cours, mars 2004.

Appendice A. Considérations de mise en œuvre

A.1 Liens d'antémémoire SPD aux entrées de SAD sortantes

Le paragraphe 4.4.2 de la [RFC4301] dit que "pour le traitement sortant, chaque entrée de SAD est pointée par les entrées dans la partie SPD-S de l'antémémoire de SPD". Le document ne spécifie pas comment ce "pointage" est fait exactement, car ceci est un détail de mise en œuvre qui n'a pas à être normalisé.

Cependant, il est clair que les liaisons entre les antémémoires de SPD et la SAD doivent être faites correctement pour assurer que les paquets sortants sont envoyés sur la bonne SA. Certaines mises en œuvre sont connues pour avoir des problèmes dans ce domaine.

En particulier, mémoriser simplement la paire (adresse IP d'en-tête de tunnel distant, SPI distant) dans l'antémémoire de SPD n'est pas suffisant, car la paire n'identifie pas toujours de façon univoque une seule entrée de SAD. Par exemple, deux hôtes derrière le même NAT peuvent se trouver accidentellement choisir la même valeur de SPI. La situation peut aussi se produire quand un hôte se voit allouer une adresse IP qui a été précédemment utilisée par un autre hôte, et que les SA associées à l'ancien hôte n'ont pas encore été supprimées par la détection d'homologue mort. Cela peut conduire à ce que des paquets soient envoyés sur la mauvaise SA ou, si l'automate de gestion de clé s'assure que la paire est unique, de refuser la création de SA par ailleurs valides.

Mémoriser l'adresse IP d'en-tête de tunnel distant dans l'antémémoire de SPD peut aussi compliquer la mise en œuvre de MOBIKE, car l'adresse peut changer durant la durée de vie de la SA. Donc, on recommande de mettre en œuvre les liaisons entre l'antémémoire de SPD et la SAD d'une façon qui n'exige pas de modification quand l'adresse IP d'en-tête de tunnel est mise à jour par MOBIKE.

A.2 Création de SA sortantes

Quand un paquet sortant exige le traitement IPsec mais qu'il n'existe pas de SA convenable, une nouvelle SA va être créée. Dans ce cas, l'hôte doit déterminer (1) qui est le bon homologue pour cette SA, (2) si l'hôte a déjà une SA IKE avec cet homologue, et (3) si aucune SA IKE n'existe, la ou les adresses IP de l'homologue pour le contacter.

Ni la [RFC4301] ni MOBIKE ne spécifient exactement comment ces trois étapes sont menées à bien. Le paragraphe 4.4.3.4 de la [RFC4301] dit :

Par exemple, supposons que IKE A reçoive un paquet sortant destiné à l'adresse IP X, un hôte desservi par une passerelle de sécurité. La [RFC2401] et le présent document ne spécifient pas comment A détermine l'adresse de l'homologue IKE qui dessert X. Cependant, tout homologue contacté par A comme représentant présumé de X doit être enregistré dans la PAD afin de permettre que l'échange IKE soit authentifié. De plus, quand l'homologue authentifié affirme qu'il représente X dans son échange de sélecteur de trafic, le PAD va être consulté pour déterminer si l'homologue en question est autorisé à représenter X.

Dans l'étape 1, il peut y avoir plus d'un homologue possible (par exemple, plusieurs passerelles de sécurité qui sont permises pour représenter X). Dans l'étape 3, l'hôte peut avoir besoin de consulter un répertoire tel que le DNS pour déterminer la ou les adresses IP de l'homologue.

Quand elles effectuent ces étapes, les mises en œuvre peuvent utiliser les informations contenues dans la SPD, la PAD, et éventuellement quelque autre base de données spécifique de la mise en œuvre. Sans considération de la façon exacte dont les étapes sont mises en œuvre, il est important de se souvenir que les adresses IP peuvent changer, et qu'une adresse IP seule n'identifie pas toujours de façon univoque un seul homologue IKE (pour la même raison que la combinaison de l'adresse IP distante et du SPI n'identifient pas de façon univoque l'identité d'une SA IPsec sortante ; voir l'Appendice A.1). Donc, dans les étapes 1 et 2 il peut être plus facile d'identifier le "bon homologue" en utilisant son identité authentifiée plutôt que l'adresse IP courante. Cependant, ces détails de mise en œuvre sortent du domaine d'application de la présente spécification.

Adresse de l'auteur

Pasi Eronen (éditeur)
Nokia Research Center
P.O. Box 407
FIN-00045 Nokia Group
Finlande

mél : pasi.eronen@nokia.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.